Agenda

• About Us
• How did we get the malware?
• Analysis Outline
• Sample A – Casino Club in Las Vegas
• Sample B – Hotel in New York
• Sample C – Video Poker in Lake Tahoe
• Sample D – Restaurant in Michigan
• Conclusions
• Tools We Like
• Contacts
About Us

Nicholas J. Percoco, Head of SpiderLabs @ Trustwave - 14 Yrs

Jibran Ilyas, Senior Forensic Analyst @ Trustwave - 5 Yrs

SpiderLabs is the advance security team at Trustwave responsible for incident response, penetration testing and application security tests for Trustwave’s clients.

SpiderLabs has responded to hundreds of security incidents, performed thousands of penetration tests and security tested hundreds of business applications for Fortune 500 organizations.
How did we get the Malware?

In 2008, we visited 150 different environments that were compromised via a number of different methods. Specifically, we saw a huge increase in Malware (targeted or mainstream) based attacks.

The basic method of acquisition was visit the location, live analysis, memory dumps, and disk imaging.

After we had a copy of the sample, it was taken back to SpiderLabs for further analysis. SpiderLabs has two physical laboratories - Chicago and London.

The contents of this talk is a walk through of what found to be some of more interesting samples we have in our collection going from simple and common to rare and complex.
Analysis Outline

During this presentation we are going to present each case in the following way:

- **Architecture and Problems**
  - What did the Target Environment look like?

- **Tools Found**
  - What did the attackers leave behind?

- **Installation Vector**
  - How did it end up in the Target Environment?

- **Static Analysis / Dynamic Analysis**
  - A deeper look at the Malware with and without executing it.

- **Data Exfiltration / Propagation**
  - What damage did it do?

- **Live Demo**
  - The malware in action - live in a VM environment.
Sample A:

Casino Club in Las Vegas
Firewall (Allowing RDP – Port 3389)

Back of House Server (No Egress filtering)

POS Terminals (No Internet Access Permitted)
Sample A – Problems

• Remote Desktop allowed from Internet to Club POS Server

• Weak / Common passwords
  – E.g. <pos name> : <pos name>
  – <pos name user> : <pos name user>
  – Beauty of life lies in simplicity

• Antivirus had not been updated since last POS software upgrade i.e. 8 months

• Customer data carried from two previous owners of the systems.
  – Data was not wiped between owners!!!!

• Casino’s network was very flat and lacked “physical” network security controls.
## Sample A – Tools Found

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>MD5 Hash</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX[1].EXE</td>
<td>680KB</td>
<td>7c0444811ef6a9ad8551215707ccecfa9</td>
<td>Unprotected SFX archive containing Keylogger and Putty</td>
</tr>
<tr>
<td>PUTTY.EXE</td>
<td>444KB</td>
<td>9BB6826905965C13BE1C84CC0FF83F42</td>
<td>Putty (SSH Client)</td>
</tr>
<tr>
<td>XXX.EXE</td>
<td>424KB</td>
<td>994FFAE187F4E567C6EFEE378AF66AD0</td>
<td>Main Keylogger executable</td>
</tr>
<tr>
<td>A0045175.exe</td>
<td>1,969KB</td>
<td>cd6d403474e7c94a7ea81ce652d8ccf8</td>
<td><strong>SMTP Server</strong> <em>(original name 1st.exe)</em></td>
</tr>
</tbody>
</table>
Sample A – Installation Vector

- Entry via Remote Desktop from IP in United States (216.15.X.X)
  - Targeted account was “posuser”

- Downloaded an unprotected SFX archive from FTP site in United States (drugzseller.xxxxx.com)

- SFX Archive had Keylogger and Putty executable

- Purchased and Installed SMTP Server on Club POS server
  - Remember POS Terminals not allowed to access the Internet, thus Club POS server used as the outbound SMTP proxy

- Used VNC to get to POS Terminals and install Keylogger
## Sample A – Installation Vector

### Attacker’s server with tools

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td>14-Sep-2008 07:09</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>IST.exe</td>
<td>14-Sep-2008 07:27</td>
<td>3.9M</td>
<td></td>
</tr>
<tr>
<td>7z.tgz</td>
<td>29-Oct-2008 09:03</td>
<td>239k</td>
<td></td>
</tr>
<tr>
<td>ACARET.exe</td>
<td>14-Sep-2008 07:27</td>
<td>665k</td>
<td></td>
</tr>
<tr>
<td>MSVC60.DLL</td>
<td>14-Sep-2008 07:27</td>
<td>392k</td>
<td></td>
</tr>
<tr>
<td>Q.exe</td>
<td>24-Oct-2008 10:51</td>
<td>1.8M</td>
<td></td>
</tr>
<tr>
<td>TOY.exe</td>
<td>14-Sep-2008 07:28</td>
<td>122k</td>
<td></td>
</tr>
<tr>
<td>T3.exe</td>
<td>14-Sep-2008 07:28</td>
<td>166k</td>
<td></td>
</tr>
<tr>
<td>UltraVNC-102-Setup.exe</td>
<td>14-Sep-2008 07:24</td>
<td>1.7M</td>
<td></td>
</tr>
<tr>
<td>X.exe</td>
<td>26-Oct-2008 05:43</td>
<td>166k</td>
<td></td>
</tr>
<tr>
<td>Xl.exe</td>
<td>09-Oct-2008 12:40</td>
<td>166k</td>
<td></td>
</tr>
<tr>
<td>X2.exe</td>
<td>25-Sep-2008 19:55</td>
<td>166k</td>
<td></td>
</tr>
<tr>
<td>X3.exe</td>
<td>06-Oct-2008 22:54</td>
<td>166k</td>
<td></td>
</tr>
<tr>
<td>XXX.exe</td>
<td>14-Sep-2008 07:24</td>
<td>472k</td>
<td></td>
</tr>
<tr>
<td>rdp.tgz</td>
<td>14-Sep-2008 07:29</td>
<td>302k</td>
<td></td>
</tr>
<tr>
<td>tmp/</td>
<td>02-Oct-2008 13:32</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>urar30b5.exe</td>
<td>14-Sep-2008 20:06</td>
<td>1.2M</td>
<td></td>
</tr>
</tbody>
</table>
Sample A – Installation Vector

The following is a summary of your order. Please review the details and then click on the Complete Transaction button to complete the checkout process.

Cardholder Details
- Name: Betty
- Company Name: 
- Street Address: 214
- City: Monroe
- State/Province: MO
- Zip/Postal Code: 65
- Country: United States
- E-Mail Address: drugseller2@*
- Alternative E-Mail: 

Transaction Details
- Card Number: (Last 4 digits) 0658
- Expiry Date: 04/09
- Security Code: ***
- Issue Number: 
- Card Type: Visa
- Order Number: U30072404

Product Code | Name          | Comments | Price  | License Pack                  | Quantity | Net Total
-------------|---------------|----------|--------|--------------------------------|----------|--------
4507 SMTP    | 1st SMTP Server | Single   | US $69.00 | 1 - User License Keycode by email | 1        | US $69.00

Net Total: US $69.00
Grand Total: US $69.00

Attacker buying SMTP server while on Club POS Server
Sample A – Dynamic Analysis

XXX.EXE

- Installed in C:\Program Files\outlook folder of the system
  - Other possible locations include:
    - C:\Windows\Security
    - C:\Windows\System32
    - C:\Program Files\BPK

- Uses Keylogger’s properties to hide from task manager, start menu and system tray; uses a keyboard combination to unlock

- Creates a BPK.dat file which can be opened only by Keylogger’s log viewer; contains full credit card track data

- Keylogger also takes screenshots of system at regular intervals; doesn’t spare attacker activity either
Sample A – Dynamic Analysis

XXX.EXE

Targets

Enable logging in all applications
Enable logging in the following application only:

Specify an application where you want Perfect Keylogger enabled:

By application

Internet Explorer C:\Program Files\Internet Explorer\IE...
Outlook Express C:\Program Files\Outlook Express\ms...
ICQLite C:\Program Files\ICQLite2006\ICQLite...

Add... Modify... Delete...
Sample A – Data Exfiltration

Data was collected in BPK.DAT file

Data was exported via SMTP server to montana2XXXXXXX@xxxx.com
Sample A – Data Exfiltration

Thursday, 30 October

Xxx.exe, 4:10 AM
BlazingTools Perfect Keylogger: Options
[Password captured: 1]
ftp.drugseller
[Password captured: 1]
drugsseller
[Password captured: 1]

Xxx.exe, 4:14 AM
BlazingTools Perfect Keylogger: Options
[Password captured: 1qaz2wsx]

Xxx.exe, 4:14 AM
PKL Window
COPYING TO THE CLIPBOARD WAS LOGGED:
OKND-FCG8X

explore.exe, 4:14 AM
http://www.msn.com/ - Microsoft Internet Explorer
www.google.com
download putty.exe

Xxx.exe, 4:15 AM
Specify deployment package options
c:\
P
rogram
F
iles\outlook
Sample A – Propagation

- The attacker used VNC to get to the POS Terminals
  - Installed the Keylogger and configured settings to only capture keystrokes from a single process
  - Process was for POS credit card transactions
- Since there was no Internet Access allowed on POS Terminals, the data was sent via SMTP server installed on Club POS Server
Sample A – Live Demo

XXX.EXE
Sample A – Add’l Comments

- This attack vector was used for hundreds of bars/restaurants
  - Commonality was the accessibility of remote access programs and weak passwords

- These are not usually detected because there are no IT personal regularly monitoring the systems or alerts miss

- The Keylogger survived several upgrades and system audits as it was hidden from task manager, system tray and start menu
  - Also, the dat file was readable only by the Keylogger program

- Keyloggers are good; too good for even the attackers
Sample B:

Hotel in New York
Sample B – Problems

• The firewall was a consumer router – allowed RDP inbound to many systems.

• Hotel Management System and POS Terminals running Windows that had not been patched since their installation (2004 & 2006).

• Weak username and passwords (many BLANK) for local system and domain accounts including Administrator (password:nimda)

• No Anti-Virus or Anti-Malware on ANY of the systems in the environment.

• No network segmentation for any of the systems or networks in the hotel.
<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>MD5 Hash</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAR.EXE</td>
<td>573K</td>
<td>ee7d411f47b13fb204a188fc37e7fc61</td>
<td>FAR is a collection of productivity tools combining advanced find/replace, HTML Help 1.x &amp; MS Help 2.x authoring, FTP, File and ZIP functions in a single interface.</td>
</tr>
<tr>
<td>ENT.EXE</td>
<td>350K</td>
<td>defd991b647811e8e8e5591365e3be41</td>
<td>ENT is a set of network scanning, security and admin tools useful in diagnosing networks and monitoring network connections.</td>
</tr>
<tr>
<td>GET2.EXE</td>
<td>48K</td>
<td>73ba6f159e752705ed2cde6953769a9b</td>
<td>GET2 Penetrator Version 1.9.9d - Windows Authentication information exfiltrator</td>
</tr>
<tr>
<td>SL.EXE</td>
<td>20K</td>
<td>3a97d9b6f17754dcd38ca7fc89caab04</td>
<td>Yep, Foundstone’s ScanLine 1.01 tool.</td>
</tr>
<tr>
<td>SERVER.EXE</td>
<td>868K</td>
<td>e02d4cc6ec3b7907b35d9456ab092da3</td>
<td>This is obfuscated version of an application called REDIR.EXE, a proxy application used to redirect incoming connections.</td>
</tr>
<tr>
<td>SVCHOST.EXE</td>
<td>596K</td>
<td>ee23d3c0de12c1644f0ed8abc818aca1</td>
<td>File transfer, anti-debugging</td>
</tr>
<tr>
<td>WINMGMT.EXE</td>
<td>65K</td>
<td>3e19ef9c9a217d242787a896cc4a5b03</td>
<td>Memory Dumper and Track Data Parser loader</td>
</tr>
<tr>
<td>CSRSVC.EXE</td>
<td>74K</td>
<td>1f9d0d200321ad6577554cc1d0bb6b69</td>
<td>Customized Memory Dumper</td>
</tr>
<tr>
<td>DNSMGR.EXE</td>
<td>1,135K</td>
<td>bf27e87187c045e402731cdaa8a62861</td>
<td>Track Data Parser</td>
</tr>
</tbody>
</table>
Sample B – Installation Vector

- Initial entry via Remote Desktop
- Targeted accounts were Administrator (pwd = nimda), Backup (pwd = veritas), SQLDebugger (pwd = user01)
- Download of Attacker toolkit (protected SFX archive)
- Malware was extracted on target computer and remote deployment via Microsoft’s “psexec.exe” to other systems on local and corporate network.
SVCHOST.EXE

- Runs as a Windows Service
- Used to establish connection to remote server in South Korea over SSL
- Anti-Debugging Built In:
  - When run from Explorer it tries to...
    1. Lock the Workstation
    2. Perform a System Shutdown
    3. Terminate All Processes
    4. Close All Terminal Sessions
    5. Toss the Workstation in Standby Mode
- It checks to see if the Windows Service is running in a virtual environment such as VMWare, Virtual PC, Qemu, VirtualBox.
- If so, it executes the above shutdown / system kill processes
- All strings in the binary are encrypted
Decrypted Strings also contain a Memo from the author…

“A few years ago I began to teach myself about computer science at my residence. I was initially interested in networking and security, so I developed this program. I do not currently know what I intend to do with this, but I have accepted the fact that I must do some limited experiments.”
Sample B – Static Analysis

WINMGMT.EXE

- Normal Windows Binary; Not Obfuscated.
- Strings Analysis show:
  - The malware utilizes Windows Service Control Management
- References to Winsock API
- FTP Commands (USER, PASS, TYPE 1, 331, 230, etc.)
- Regular Expressions for Track 1 and Track 2 data:
  
  \(((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^[0-9]{7-9}[10-5]\((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})
  
  \(([0-9]{15,16}[D=][0-9]{7-9}[10-5]\((0[1-9])|(1[0-2]))[0-9\s]{8,30}\))
Sample B – Dynamic Analysis

WINMGMT.EXE

- Executing from command line or Explorer produces Error 1063.
- Using “/install” does the trick.
- It can run in debug mode
- **Once running it locates one of eight Point of Sale system process it is designed to monitor.**
- As cards are swiped on monitored processes, it creates process memory dump file in “memdump” folder and then calls a process called “dnsmgr.exe” which parses track data from dump files to an ASCII file “dirmon.chm”
Sample B – Data Exfiltration

- The attacker’s created RAR archives created with WinRar and password protected them.
  - We obtained the passwords for these RAR files by searching RAM dumps from the compromised systems and parsing for interesting strings
  - Found “!SYSTEMNAME#623!” and it worked!

- Data exported via over SSL to a host in South Korea (211.232.XXX.X).

- Estimated that 350,000 (or more) credit cards were exported during the time the attackers were on the systems. This is based upon the contents of the RAR files.
Sample B – Propagation

- The attackers made connection using RDP to 35 other hotel locations via the corporate WAN.

- We visited many of the other locations and found the exact same sets of tools and large quantities of RAR files containing credit card data.
Sample B – Live Demo

WINMGMT.EXE
Sample B – Add’l Comments

Why isn’t this malware caught?

• Anti-Virus can’t catch this
  – They only know what they know.

• Lack of Log Review

• No checks for storage of prohibited data; often a sign that someone is on the system doing something they shouldn’t be

• Thanks to the IT Talent
  – On few of these cases, IT simply searched Google for the malware name. Needless to say the results.
Sample C:

Video Poker in Lake Tahoe

Note: This portion of the talk is based on actual cases we investigated where the use of “credentialed” malware was found. This portion of the presentation does not discuss or infer that any specific Video Poker system is vulnerable to this attack method.
Sample C – What is Credentialed Malware?

Credentialed Malware:

• A program that is specifically design to exploit functions of the target application that are not typically available to the normal end user.

• Access to the malware’s functions are control by the developer using various forms of “authentication” tokens.

• Authentication Tokens could be sold or rented to criminals looking to illegally obtain what ever the target application is in the business of providing.
A – Video Poker Machine
B – Voucher Reader / Printer
C – Casino Network
D – The Casino
Sample C – Common Problems

- Due to the number of machines and maintenance required, machines are constantly being worked on.
  - Does the “Eye in the Sky” monitor repair personnel?
- Unique passwords are difficult to manage.
- Do you need to run AV on Video Poker machines?
- Under the hardened case they are low end PCs and may have USB ports, etc.
- What OS are they running? How often are they patched?
Sample C – Installation Vector

Possible scenario:

- Attacker, dressed like casino repair staff, with a key walks up to the Video Poker Machine.
- They login using a default/common password (i.e. all Casino’s machines have the same password)
- The Attacker inserts a USB key with the Malware on it
- The Attacker copies the dropper over to the local file system
- The Attacker executes the dropper file, removes the USB key, and locks up the machine

Another scenario:

- The malware is installed at the manufacture as a “backdoor”
- It is active on every single Video Poker machine deployed…
Sample C – Analysis

VIDEOPOKER.EXE

• While the malware is active it parsing for valid Vouchers, it is also looking for a User Voucher:
  — **Single Function** – activates a single function execution
  — **Multi-Function** – activates the malware interface window

• A User Voucher is identified by passing the value of the Voucher through a hashing algorithm and comparing the results to set values stored in the malware.

• If the malware does NOT see a User Voucher, it does nothing and passes the information over to the Video Poker software for adding credits to the game.
## Sample C – Analysis

**VIDEOPOKER.EXE**

<table>
<thead>
<tr>
<th>Key Value</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold (1)</td>
<td>Uninstall</td>
<td>Deletes the malware service, puts the system logs back where they were before the malware was installed.</td>
</tr>
<tr>
<td>Hold (2)</td>
<td>Display Stats</td>
<td>Presents information on the number of User Vouchers uses (function 3 and 4) and malware version running on the machine.</td>
</tr>
<tr>
<td>Hold (3)</td>
<td>Odds Shift</td>
<td>Modifies the odds on the machine by increasing the face cards in ‘deck’.</td>
</tr>
<tr>
<td>Hold (4)</td>
<td>Modify Credits</td>
<td>Prompts ‘user’ to enter value of credits (using 1,2,3,4,5 Hold keys), adds the value to the current game, and then can be cashed out.</td>
</tr>
<tr>
<td>Deal</td>
<td>Test Printer</td>
<td>Prints ‘hello world’ to the voucher printer.</td>
</tr>
<tr>
<td>Max Bet</td>
<td>Exit</td>
<td>Exits the malware and returns to normal game play. Also, used to enter a value to get to a sub-function.</td>
</tr>
</tbody>
</table>
Sample C – Propagation

- If the Video Poker machine is connected to the Casino network (and likely will be) a services based vulnerability would be needed.

- The attackers could check for successful propagation by walking up to random machines. Inserting a User Voucher that will either result in it being rejected or the activation of the Malware.
Sample C – Live Demo

VIDEOPOKER.EXE
Sample D:

Restaurant in Michigan
Sample A - Architecture

- POS Terminals (Internet Access Permitted)
- Firewall / Linksys Router (Allowing VNC – Port 5900)
- Back of House Server (No Egress filtering)
Sample D – Problems

- VNC allowed from Internet to Restaurant POS Server

- Weak / Common passwords
  - E.g. Admin: support

- POS Terminals were not running Anti Virus software

- Unrestricted Internet Access was allowed from all systems including POS Terminals

- POS Integrator used same passwords for all restaurants in the region
## Sample D – Tools Found

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>MD5 Hash</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOST32EDU.EXE</td>
<td>68KB</td>
<td>17c83eba9a436edbeb74a42a51b9087a</td>
<td>IRC Bot / Backdoor</td>
</tr>
<tr>
<td>X.BAT</td>
<td>2KB</td>
<td>N/A</td>
<td>Malware loader</td>
</tr>
<tr>
<td><em>contents of file found in Unallocated Clusters</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REPZ.EXE</td>
<td>65KB</td>
<td>6c9e01933aa88894f476d690666dc483</td>
<td>IRC Bot / Backdoor</td>
</tr>
<tr>
<td>PACKETSNIFFER.EXE</td>
<td>57KB</td>
<td>10e5a2813d51c547346173290a0ae53b</td>
<td>Packet Sniffer</td>
</tr>
</tbody>
</table>
Sample D – Installation Vector

- Entry via VNC on POS Server
  - VNC password was “support”

- Downloaded malware files
  - IRC Bot
  - X.bat (Malware loader)
  - Custom Packet Sniffer

- Malware kills all security software in Windows

- Microsoft .Net framework version 2.0 was downloaded as Packet Sniffer was written in .Net and needs the framework to run properly.

- IRC Bot downloads the configuration (tcp ports, output file location, etc.) for the system based on POS software installed

- Sniffed files are placed in C:\Export folder and then uploaded to FTP server.
Sample D – Dynamic Analysis

PACKETSNIFFER.EXE

- Installed in C:\Windows\Temp folder of the system
- Uses Microsoft .Net Framework v2.0 to run properly
- Uses a configuration file, which is created based on POS software
- Sniffs TCP traffic on ports 5101,5010,5011,5100
- Stores the sniffed output in C:\Export folder
  - Filenames are <ip address>.SEND.cap and <ip address>.READ.cap
- Data is uploaded to an IP based in Munich, Germany
Sample D – Live Demo

PACKETSNIFFER.EXE
Sample D – Add’l Comments

• The destination FTP server for sniffed output files contained several other folders; all of which had sniffer output files.

• Upon analysis of FTP server, it was concluded that 9 other restaurants were affected by the same sniffer and they were all sending the data regularly to the FTP server.

• 6 of the restaurants were all are based in Michigan; all restaurants are serviced by same POS Integrator.
Conclusions

• Malware is dominating

• Computer Memory is the target to extract sensitive data

• Companies are still not getting segmentation, passwords, firewalls right!! Easy Entry.

• Attackers are taking the time to learn, even obscure business applications before creating targeted Malware.

• Once Malware use has proved successful, similar businesses and environments are targeted quickly.
<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependency Walker</td>
<td><a href="http://www.dependencywalker.com">http://www.dependencywalker.com</a></td>
<td>Lists the imported and exported functions of an executable file</td>
</tr>
<tr>
<td>Encase</td>
<td><a href="http://www.guidancesoftware.com">http://www.guidancesoftware.com</a></td>
<td>Forensic Analysis and Case Management</td>
</tr>
<tr>
<td>FastDumpPro</td>
<td><a href="http://www.hbgary.com/products-services/">http://www.hbgary.com/products-services/</a></td>
<td>Memory Acquisition Tool</td>
</tr>
<tr>
<td>FTK Imager Lite</td>
<td><a href="http://www.accessdata.com/">http://www.accessdata.com/</a></td>
<td>Acquires Windows Images Live</td>
</tr>
<tr>
<td>GMER</td>
<td><a href="http://www.gmer.net">http://www.gmer.net</a></td>
<td>Detect hidden processes and rootkits</td>
</tr>
<tr>
<td>Hex Workshop</td>
<td><a href="http://www.hexworkshop.com">http://www.hexworkshop.com</a></td>
<td>Analyze, edit, cut, copy, paste, insert, fill and delete binary data</td>
</tr>
<tr>
<td>IDA Pro</td>
<td><a href="http://www.hex-rays.com/idapro">http://www.hex-rays.com/idapro</a></td>
<td>Disassembler and Debugger</td>
</tr>
<tr>
<td>NMAP</td>
<td><a href="http://www.nmap.org">http://www.nmap.org</a></td>
<td>Network Port Scanner</td>
</tr>
<tr>
<td>RegRipper</td>
<td><a href="http://regripper.net">http://regripper.net</a></td>
<td>Registry Analysis</td>
</tr>
<tr>
<td>Regshot</td>
<td><a href="http://sourceforge.net/projects/regshot">http://sourceforge.net/projects/regshot</a></td>
<td>Acquires and Compares registry snapshot</td>
</tr>
<tr>
<td>Volatility</td>
<td><a href="https://www.voltilesystems.com/default/volatility">https://www.voltilesystems.com/default/volatility</a></td>
<td>Memory Analysis</td>
</tr>
<tr>
<td>Win32dd</td>
<td><a href="http://win32dd.msuiche.net">http://win32dd.msuiche.net</a></td>
<td>Memory Acquisition Tool</td>
</tr>
<tr>
<td>Wireshark</td>
<td><a href="http://www.wireshark.org">http://www.wireshark.org</a></td>
<td>Network Protocol Analyzer</td>
</tr>
</tbody>
</table>
Contact Us

Contacts:

Nicholas J. Percoco <npercoco@trustwave.com> / @c7five

Jibran Ilyas <jilyas@trustwave.com>

www.trustwave.com/spiderlabs/ @SpiderLabs

Special Thanks:
Adam, Stephen, Colin, Chris, Ferns, Brandon, and Nathan.